REMARKS

In the Office Action mailed April 17, 2008 (hereinafter "Office Action"), Claims 1-9, 11-38, and 60-63 were rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent Publication No. 2004/0103310, by Sobel et al. (hereinafter "Sobel"). Claim 10 was rejected under 35 U.S.C. § 103(a) as unpatentable over Sobel. Claims 39-47, 51, 53, and 56 were rejected under 35 U.S.C. § 103(a) as unpatentable over Sobel in view of U.S. Patent Publication No. 2003/0065942, by Lineman et al. (hereinafter "Lineman"). Claims 39, 41-53, and 56 were also rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent Publication No. 2004/0107360, by Herrmann et al. (hereinafter "Herrmann"), in view of Lineman. Applicants respectfully disagree with these rejections, but have amended the claims to further advance prosecution of the present application.

With this response, Claims 1-3, 7-9, 12, 14, 15, 18, 21-23, 25, 26, 28-30, 33-35, 39, 51, and 60-62 are amended. Claims 11, 13, 16, 24, and 46 are canceled. Accordingly, Claims 1-10, 12, 14, 15, 17-23, 25-45, 47-51, 53, 56, and 60-63 are currently pending in the present application. Applicants have carefully considered the issues raised in the Office Action and request reconsideration and allowance of the claims in view of the remarks set forth below.

Patentability of Independent Claims 1, 15, 26, 33, and 39

The Office Action rejected independent Claims 1, 15, 26, and 33 under 35 U.S.C. § 102(e) as anticipated by Sobel, and rejected independent Claim 39 under 35 U.S.C. § 103(a) as unpatentable over Sobel in view of Lineman, and over Herrmann in view of Lineman. Applicants respectfully disagree, but have amended the independent claims to clarify the recited matter and to further advance prosecution of the present application.

As amended, Claim 1 recites:

> 1. A method for providing security in a computer system *by a clean group server*, comprising:

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

specifying a set of properties for use in determining if an item is clean;

in response to receiving an add request from an item, the *add request containing evidence collected from the item* relating to the presence or absence of the properties in the specified set of properties, *evaluating the add request* to determine if the evidence proves that the item has the specified set of properties; and

determining from the evidence in the add request whether the item has the specified set of properties, and if so, designating the item as a member of a clean group by *instructing a domain controller to add the item to the clean group, the domain controller configured to store information identifying network users and resources*. (Emphasis added.)

As amended, Claim 15 recites:

15. A system for managing security, comprising:

a clean group server;

a domain controller configured to store information identifying network users and resources, including a clean group indicating a group of computers and users that are more trusted than computers and users not included in the clean group;

a clean runtime component, the clean runtime component being installed on an item and being able to communicate with the clean group server; and

the clean runtime component configured to send an add request to the clean group server, the *add request including evidence to be evaluated by the clean group server* for determining whether to add the item to a clean group;

wherein the clean group server is configured to determine whether the evidence sent by the clean runtime component is sufficient to prove that the item is in compliance with a security policy, and if so, to designate the item as a member of the clean group by *instructing the domain controller to add the item to the clean group*. (Emphasis added.)

As amended, Claim 26 recites:

26. One or more computer-readable media having computer-executable components for providing security in a computer system, the computer-executable components comprising:

a clean runtime object for installation on a computer, wherein the clean runtime object, when executed, performs a compliance check to determine if the computer has a specified set of properties, and sends an

add request containing evidence relating to whether the computer has the specified set of properties to a clean group server; and

instructions for installation on a clean group server for processing the add request, wherein the instructions, when executed, cause the clean group server to instruct *a domain controller configured to store information identifying network users and resources* to add the computer as a member of a clean group upon receipt of an add request, *if the clean group server determines that the add request contains sufficient evidence to prove that the computer has the specified set of properties*. (Emphasis added.)

As amended, Claim 33 recites:

33. A method for providing security in a computer system, comprising:

specifying a set of properties for use in determining if a computer is clean;

evaluating a computer to determine if it has the specified set of properties;

sending an add request to a clean group server; and

based on whether or not *the clean group server determines that the computer is in compliance, the clean group server disabling or enabling the computer domain account on a domain controller, the domain controller configured to store information identifying network users and resources*. (Emphasis added.)

As amended, Claim 39 recites:

39. A method for providing security in a computer system, comprising:

performing compliance checks for items;

placing items which pass the compliance check into a clean group by communicating with a domain controller, the *domain controller configured to store information identifying network users and resources*; and

removing items from the clean group which fail the compliance check;

wherein items within the clean group can access a collection of IPSec communication requirements and parameters that allow them to communicate with other items within the clean group; and

items not within the clean group cannot access the collection of IPSec communication requirements and parameters, and are thereby quarantined from receiving information from or sending information to items within the clean group. (Emphasis added.)

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Applicants respectfully submit that Sobel, Lineman, and Herrmann, both alone and in combination, fail to teach, describe, or suggest the combination of features recited in independent Claims 1, 15, 26, 33, and 39, including a clean group that is managed by a *domain controller configured to store information identifying network users and resources*, as recited in amended Claims 1, 15, 26, 33, and 39; or *a clean group server* that receives an add request containing *evidence* to be evaluated *by the clean group server* to determine whether an item has a specified set of properties as substantially recited in amended Claims 1, 15, 26, and 33.

First, applicants respectfully submit that Sobel, Lineman, and Herrmann all fail to teach, describe, or suggest a clean group that is managed by *a domain controller configured to store information identifying network users and resources*. The Office Action asserts in paragraph 5 that the DHCP server of Sobel anticipates the broadest possible interpretation of the recited "domain controller," before amendment. Applicants respectfully disagree, and respectfully submit that one of ordinary skill in the art would understand a domain controller to be distinct from a DHCP server, and a "domain" to be distinct from the separate protected and restricted networks of Sobel. Applicants respectfully submit that one skilled in the art would understand a "domain controller" to be a server containing information that identifies network users and resources. *See* Microsoft Computer Dictionary, p. 172 (5th ed. 2002). Nevertheless, applicants have amended Claims 1, 15, 26, 33, and 39 to further clarify the recited subject matter. Applicants respectfully submit that the DHCP server of Sobel fails to teach, describe, or suggest a domain controller configured to *contain information that identifies network users and resources* as recited in amended Claims 1, 15, 26, 33, and 39.

Herrmann similarly fails to teach, describe, or suggest a *domain controller configured to store information identifying network users and resources*. The Office Action cites to Figure 4, reference numbers 320, 330, 440, 450, and 460 as disclosing a domain controller. Applicants respectfully disagree that this discloses or suggests a domain controller as recited in amended

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Claims 1, 15, 26, 33, and 39. Indeed, reference numbers 320, 330, 440, 450, and 460 simply coordinate to decide at a low level whether to give the client device 310 access to the protected network or resources 390. Applicants respectfully submit that this function does not teach or suggest the *storing of information identifying network users and resources*, as the domain controller of Claims 1, 15, 26, 33, and 39 is configured to do. Applicants respectfully submit that Lineman also fails to teach or suggest a domain controller as recited in amended Claims 1, 15, 26, 33, and 39.

In addition, applicants respectfully submit that Sobel, Lineman, and Herrmann, both alone and in combination, fail to teach, describe, or suggest *a clean group server* that receives an add request containing *evidence* to be evaluated *by the clean group server* to determine whether an item has a specified set of properties as substantially recited in amended Claims 1, 15, 26, and 33. The Office Action asserts that the Compliance Registration Manager and DHCP Proxy of Sobel are functionally equivalent to the clean group server. Office Action, paragraph 4. Applicants respectfully disagree that Sobel teaches, discloses, or suggests the features of amended Claims 1, 15, 26, and 33, because the Compliance Registration Manager and DHCP Proxy, as well as the rest of Sobel, fail to teach, disclose, or suggest the method steps as recited in amended Claims 1, 15, 26, and 33, including receiving an add request containing evidence to be evaluated *by the clean group server* to determine whether an item has a specified set of properties. In Sobel, compliance with a security policy is determined by the compliance registration manager 135 on the client. *See* Sobel, Fig. 2, reference numbers 210, 215; paras. 18, 20 ("The system includes a compliance verification component 190, which can be implemented as a computer program that runs *on the client* 105.... *[T]he compliance verification component 190 determines 210* whether the client is in compliance with the security policies." (emphasis added)). Even if the Compliance Registration Manager and DHCP Proxy of Sobel disclose a clean group server (which applicants explicitly deny), Sobel does not disclose or

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

suggest that the Compliance Registration Manager or the DHCP Proxy perform any further checking of the client's compliance with the security policies after receiving the message from the compliance verification component on the client indicating compliance has been found. *See* Sobel, para. 21. The method recited in amended Claims 1, 15, 26, and 33, in which it is the *clean group server* which makes the determination of whether the item is in compliance, is superior at least because it helps ensure consistent and reliable configurations and reduces security management complexity by centralizing decisionmaking and control. Applicants respectfully submit that Herrmann and Lineman similarly fail to disclose these features of amended Claims 1, 15, 26, and 33.

Accordingly, applicants respectfully submit that independent Claims 1, 15, 26, 33, and 39 are allowable, and respectfully request withdrawal of the 35 U.S.C. § 102(e) and 35 U.S.C. § 103(a) rejections and allowance of the claims.

Patentability of Dependent Claims 2-10, 12, 14, 17-23, 25, 27-32, 34-38, 40-45, 47-51, 53, 56, and 60-63

Claims 2-10, 12, 14, 60, 62, and 63 depend from Claim 1. Claims 17-23, 25, and 61 depend from Claim 15. Claims 27-32 depend from Claim 26. Claims 34-38 depend from Claim 33. Claims 40-45, 47-51, 53, and 56 depend from Claim 39. Applicants respectfully submit that these claims are allowable at least by virtue of these dependencies, as well as by virtue of the additional claim features set forth therein.

For instance, applicants respectfully submit that the cited patents and publications fail to teach, describe, or suggest the combination of features recited in amended Claim 51, including wherein an item is a *user*, and the clean group membership *of the user* is evaluated on the basis of whether *each of a set of computers associated with the user* is in compliance.

Accordingly, applicants respectfully request withdrawal of the rejections and allowance of these claims.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

CONCLUSION

In view of the foregoing amendments and remarks, applicants submit that claims are in condition for allowance over the cited and applied references, and respectfully request reconsideration and allowance of the same. If the Examiner has any questions or comments concerning this matter, the Examiner is invited to contact applicants' undersigned attorney at the number set forth below.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS[PLLC]

David P. Sheldon
Registration No. 62,464
Direct Dial No. 206.695.1611

DPS:lal

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100